Some new orders of Hadamard and skew-Hadamard matrices

Dragomir Ž. Đoković[1], Oleg Golubitsky[2], Ilias S. Kotsireas[3]

Abstract

We construct Hadamard matrices of orders $4 \cdot 251 = 1004$ and $4 \cdot 631 = 2524$, and skew-Hadamard matrices of orders $4 \cdot 213 = 852$ and $4 \cdot 631 = 2524$. As far as we know, such matrices have not been constructed previously. The constructions use the Goethals-Seidel array, suitable supplementary difference sets on a cyclic group and a new efficient matching algorithm based on hashing techniques.

1 Introduction

There are only 13 integers $v < 500$ for which no Hadamard matrices of order $4v$ are known, see [1, 2, 8]. In this paper we are able to remove the integer $v = 251$ from this list by constructing a Hadamard matrix of order $4 \cdot 251 = 1004$ by constructing cyclic supplementary difference sets (SDS) with parameters $(251; 125, 120, 115, 115; 224)$. Hadamard matrices of order $4 \cdot 631 = 2524$ are not known to exist, according to the table on page 278 of the second edition of the Handbook of Combinatorial Designs [1], see also [4, 6]. In this paper we construct Hadamard matrices of order $4 \cdot 631$ by constructing cyclic SDS with parameters $(631; 315, 330, 330, 330; 674)$.

Skew-Hadamard matrices of orders $4 \cdot 213$ and $4 \cdot 631$ are not known to exist either, see [10] and [3] for the list of known orders of skew-Hadamard matrices. In this paper we construct skew-Hadamard matrices of orders $4 \cdot 213$ and $4 \cdot 631$ by constructing cyclic SDS with parameters $(213; 106, 106, 105, 92; 196)$ and $(631; 315, 330, 330, 330; 674)$, respectively.

All SDSs in this paper were constructed by using the well-known method of taking base blocks to be unions of orbits of an automorphism group of the underlying cyclic group and a new efficient matching algorithm. This new algorithm turned out to be a crucial part of the discovery of these new matrices.

A Hadamard matrix of order 428 has been constructed in [9] and currently the smallest multiple of 4 for which a Hadamard matrix is not known is 668. We refer the reader to [7] and [10] for more information on Hadamard and skew-Hadamard matrices.

[1]University of Waterloo, Department of Pure Mathematics, Waterloo, Ontario, N2L 3G1, Canada e-mail: djokovic@math.uwaterloo.ca

[2]Google, Inc. 151 Charles West, Kitchener, Ontario, N2G 1H6, Canada, e-mail: oleg.golubitsky@gmail.com

[3]Wilfrid Laurier University, Department of Physics & Computer Science, Waterloo, Ontario, N2L 3C5, Canada, e-mail: ikotsire@wlu.ca

The updated list of integers $v < 500$ for which no Hadamard matrices of order $4v$ are known consists now of 12 integers

$$167, 179, 223, 283, 311, 347, 359, 419, 443, 479, 487, 491$$

all of them primes congruent to 3 (mod 4).

2 The matching algorithm

One of the serious difficulties of the unions of orbits approach when used in conjunction with the Goethals-Seidel array is that one needs to locate four lines in four text files such that the element-wise sums of these four lines are all equal to the same (pre-defined) constant. The difficulty stems from the fact that if two files contain ten million lines each, then the file with all possible sum combinations of these two files will contain 10^{14} lines and therefore the ensuing naive algorithm to solve this problem, i.e. to combine the files two by two in two pairs and look for a potential match, is utterly impractical. In order to circumvent this difficulty, one potential way to avoid this combinatorial explosion is to resort to hashing functions.

Let us begin with a precise statement of the problem we were faced with. Given four text files with M columns and N_1, N_2, N_3, N_4 lines each, one has to identify four lines, one line in each file, identified by their line numbers in each file: l_1, l_2, l_3, l_4, such that their M element-wise sums are all equal to a constant λ. In the case of the SDS $(631; 315, 330, 330, 330; 674)$ it turns out that $M = 21$, $\lambda = 674$ and that the four files contained approximately one million lines each.

Let $\mathbb{Z}_+^n$ denote the additive monoid of non-negative integer n-tuples. Given four subsets $A_1, A_2, A_3, A_4 \in \mathbb{Z}_+^n$ and a target $s \in \mathbb{Z}_+^n$, we need to find $a_i \in A_i$, $i = 1, 2, 3, 4$, such that $a_1 + a_2 + a_3 + a_4 = s$, or prove that they do not exist.

A naïve exhaustive search requires $O(\prod |A_i|)$ time and constant space. A meet-in-the-middle approach reduces this to $O(|A_1||A_2| + |A_3||A_4|)$ time but takes $O(|A_1||A_2|)$ space, by first storing all the sums $a_1 + a_2$, where $a_1 \in A_1$, $a_2 \in A_2$, in a hash set H, and then searching for $a_3 \in A_3$, $a_4 \in A_4$, such that $s - a_3 - a_4 \in H$.

For convenience, we took $B_1 = \{\lfloor \frac{s}{2} \rfloor - a_3 \mid a_3 \in A_3\}$ and $B_2 = \{\lceil \frac{s}{2} \rceil - a_4 \mid a_4 \in A_4\}$ and reduced the original problem to the equivalent one of finding $a_1 \in A_1$, $a_2 \in A_2$, $b_1 \in B_1$, $b_2 \in B_2$, such that $a_1 + a_2 = b_1 + b_2$. In our case, the elements of B_1 and B_2 turned out to be non-negative integer tuples.

In order to reduce space requirements and speed up additions, we mapped the n-tuples to 64-bit non-negative integers using a linear hash function $h : \mathbb{Z}_+^n \to \mathbb{Z}/2^{64}\mathbb{Z}$. Then we listed the solutions of $h(a_1) + h(a_2) = h(b_1) + h(b_2)$, and for each of them checked whether they yield a solution to the original problem (some of them may not because of collisions).

Furthermore, we parallelized the algorithm, reducing the overall search time and the space requirements on each worker by a factor of M, where M is the number of workers. First, we represented each of the four input sets (after hashing) as an array of lists, which at index i, $0 \leq i < M$, stores the list of all elements equal to i modulo M. Using this data structure, worker number i, $0 \leq i < M$, can easily enumerate and store in the hash set H all sums $a_1 + a_2$ equal to i modulo M, and then lookup in H all sums $b_1 + b_2$ that are also equal to i modulo M.

In practice, M was chosen to be much greater than the available number of workers, to further reduce memory use. Each worker pre-loaded the four sets in memory (represented with arrays of lists, as described above) and sequentially processed several remainders modulo M, where the number of remainders to be processed in a single run was taken large enough, so that the search time would dominate the pre-loading time, but would not exceed the maximal allowed duration of a job on the cluster. Reduced memory requirements enabled us to simultaneously schedule multiple workers on a single multi-core machine, thus fully utilizing the capacity of the cluster.

3 Results

We now present our results in the form of SDSs, for $v = 213, 251, 631$. Non-equivalence of SDSs was established by an implementation of the method described in [5].

We define the notation for the orbits of the action of the subgroup that we use to construct the solutions below. The automorphism group of the additive cyclic group Z_v will be identified with the group of invertible elements, $Z_v^\star$, of the ring Z_v. Consider a fixed subgroup H of order h of $Z_v^\star$. Clearly h must divide $|Z_v^\star| = \phi(v)$. Denote by $H \cdot k$ the orbit of H in Z_v through the point k, where $\cdot$ is multiplication $\mod v$. We refer to the orbit $H \cdot 0 = \{0\}$ as the *trivial orbit*. The orbit $H \cdot 1$ is just the subgroup H itself. In general the size of an orbit may be any divisor of $|H|$ and if v is a prime then every nonzero orbit is just a coset of H in $Z_v^\star$ and so will have size $|H|$.
The notation

$$X = \bigcup_{j \in J} H \cdot j, \quad Y = \bigcup_{k \in K} H \cdot k, \quad Z = \bigcup_{l \in L} H \cdot l, \quad W = \bigcup_{m \in M} H \cdot m \tag{1}$$

will be used below to present all the solutions found, in fact each solution will be given only via the four index sets J, K, L, M. For suitable choices of the four index sets J, K, L, M, the four sets X, Y, Z, W defined in (1) form SDS$(v; x, y, z, w; \lambda)$ with $x = \sum_{j \in J} |H \cdot j|$, $y = \sum_{k \in K} |H \cdot k|$, $z = \sum_{l \in L} |H \cdot l|$, $w = \sum_{m \in M} |H \cdot m|$ and $\lambda = x + y + z + w - v$.

All Hadamard matrices in this paper are constructed via the Goethals-Seidel array

$$\begin{bmatrix} P_1 & P_2R & P_3R & P_4R \\ -P_2R & P_1 & -P_4^TR & P_3^TR \\ -P_3R & P_4^TR & P_1 & -P_2^TR \\ -P_4R & -P_3^TR & P_2^TR & P_1 \end{bmatrix}$$

where R denotes the $v \times v$ matrix with ones in the back-diagonal and zeros everywhere else. To obtain a Hadamard matrix via the Goethals-Seidel array one has to substitute the $v \times v$ matrices P_1, P_2, P_3, P_4 by the $\{\pm 1\}$ circulant matrices that arise from the four subsets X, Y, Z, W that make up the SDS$(v; x, y, z, w; \lambda)$. More precisely, let $a_X = (a_0, \ldots, a_{v-1})$ be a sequence defined by $a_i = -1$ if $i \in X$, and $a_i = 1$ if $i \notin X$; and define the sequences a_Y, a_Z, a_W similarly. Then denote by $[X], [Y], [Z], [W]$ the $\{\pm 1\}$ circulant matrices whose first rows are a_X, a_Y, a_Z, a_W respectively. If X, Y, Z, W form a SDS$(v; x, y, z, w; \lambda)$, then

$$[X][X]^T + [Y][Y]^T + [Z][Z]^T + [W][W]^T = 4vI_v.$$

3.1 $v = 213$

Consider the subgroup $H = \{1, 37, 91, 103, 172, 187, 190\}$ of order 7, of $Z_{213}^\star$. Note that $Z_{213}^\star$ is of order $\phi(213) = 140$. Here are the 32 nontrivial orbits of the action of H on Z_{213}.

$$\begin{array}{lcllcl}
H \cdot 1 & = & [1, 37, 91, 103, 172, 187, 190] & H \cdot 21 & = & [21, 33, 93, 138, 156, 204, 207] \\
H \cdot 2 & = & [2, 74, 131, 161, 167, 182, 206] & H \cdot 22 & = & [22, 67, 85, 133, 136, 163, 175] \\
H \cdot 3 & = & [3, 60, 90, 96, 111, 135, 144] & H \cdot 23 & = & [23, 26, 41, 110, 122, 176, 212] \\
H \cdot 4 & = & [4, 49, 109, 121, 148, 151, 199] & H \cdot 28 & = & [28, 115, 124, 130, 184, 205, 208] \\
H \cdot 5 & = & [5, 8, 29, 83, 89, 98, 185] & H \cdot 30 & = & [30, 45, 48, 72, 108, 162, 174] \\
H \cdot 6 & = & [6, 9, 57, 75, 120, 180, 192] & H \cdot 34 & = & [34, 70, 94, 97, 112, 181, 193] \\
H \cdot 7 & = & [7, 31, 46, 52, 82, 139, 211] & H \cdot 38 & = & [38, 50, 77, 80, 128, 146, 191] \\
H \cdot 10 & = & [10, 16, 58, 157, 166, 178, 196] & H \cdot 39 & = & [39, 51, 105, 141, 165, 168, 183] \\
H \cdot 11 & = & [11, 68, 140, 149, 173, 188, 194] & H \cdot 42 & = & [42, 63, 66, 99, 186, 195, 201] \\
H \cdot 12 & = & [12, 18, 27, 114, 147, 150, 171] & H \cdot 43 & = & [43, 76, 79, 100, 154, 160, 169] \\
H \cdot 13 & = & [13, 55, 61, 88, 106, 118, 127] & H \cdot 44 & = & [44, 53, 59, 113, 134, 137, 170] \\
H \cdot 14 & = & [14, 62, 65, 92, 104, 164, 209] & H \cdot 69 & = & [69, 78, 102, 117, 123, 153, 210] \\
H \cdot 15 & = & [15, 24, 36, 54, 81, 87, 129] & H \cdot 71 & = & [71] \\
H \cdot 17 & = & [17, 35, 47, 56, 155, 197, 203] & H \cdot 84 & = & [84, 126, 132, 159, 177, 189, 198] \\
H \cdot 19 & = & [19, 25, 40, 64, 73, 145, 202] & H \cdot 86 & = & [86, 95, 107, 125, 152, 158, 200] \\
H \cdot 20 & = & [20, 32, 101, 116, 119, 143, 179] & H \cdot 142 & = & [142]
\end{array}$$

We give an SDS with parameters $(213; 106, 106, 105, 92; 196)$, via the index sets J, K, L, M (with respective cardinalities $16, 15, 14, 16$) to be used in (1), which gives rise to skew-Hadamard matrices of order $4 \cdot 213 = 852$. The associated decomposition into the sum of 4 squares is:

$$\begin{aligned} 4 \cdot 213 = 852 &= 1^2 + 1^2 + 3^2 + 29^2 = \\ &= (213 - 2 \cdot 106)^2 + (213 - 2 \cdot 106)^2 + (213 - 2 \cdot 105)^2 + (213 - 2 \cdot 92)^2. \end{aligned}$$

$$
\begin{array}{lcl}
J & = & \{4,5,7,10,11,15,17,19,20,30,34,38,39,42,43,142\} \\
K & = & \{2,7,12,14,17,22,28,34,39,42,43,44,69,84,86\} \\
L & = & \{1,4,11,15,17,20,21,28,30,34,42,44,69,142\} \\
M & = & \{2,4,10,11,12,15,21,22,23,28,30,34,44,69,71,86\}
\end{array}
$$

3.2 $v = 251$

Consider the subgroup $H = \{1, 20, 113, 149, 219\}$ of order 5, of $Z^{\star}_{251}$. Note that $Z^{\star}_{251}$ is of order $\phi(251) = 250$. Here are the 50 nontrivial orbits of the action of H on Z_{251}.

$$
\begin{array}{lcl lcl}
H\cdot 1 & = & [1,20,113,149,219] & H\cdot 42 & = & [42,87,162,228,234] \\
H\cdot 32 & = & [32,102,138,231,250] & H\cdot 18 & = & [18,26,109,172,177] \\
H\cdot 2 & = & [2,40,47,187,226] & H\cdot 74 & = & [74,79,142,225,233] \\
H\cdot 25 & = & [25,64,204,211,249] & H\cdot 19 & = & [19,70,129,139,145] \\
H\cdot 3 & = & [3,60,88,155,196] & H\cdot 106 & = & [106,112,122,181,232] \\
H\cdot 55 & = & [55,96,163,191,248] & H\cdot 21 & = & [21,81,114,117,169] \\
H\cdot 4 & = & [4,80,94,123,201] & H\cdot 82 & = & [82,134,137,170,230] \\
H\cdot 50 & = & [50,128,157,171,247] & H\cdot 28 & = & [28,58,108,152,156] \\
H\cdot 5 & = & [5,63,91,100,243] & H\cdot 95 & = & [95,99,143,193,223] \\
H\cdot 8 & = & [8,151,160,188,246] & H\cdot 30 & = & [30,44,98,127,203] \\
H\cdot 6 & = & [6,59,120,141,176] & H\cdot 48 & = & [48,124,153,207,221] \\
H\cdot 75 & = & [75,110,131,192,245] & H\cdot 33 & = & [33,148,158,199,215] \\
H\cdot 7 & = & [7,27,38,39,140] & H\cdot 36 & = & [36,52,93,103,218] \\
H\cdot 111 & = & [111,212,213,224,244] & H\cdot 34 & = & [34,46,77,167,178] \\
H\cdot 9 & = & [9,13,86,180,214] & H\cdot 73 & = & [73,84,174,205,217] \\
H\cdot 37 & = & [37,71,165,238,242] & H\cdot 35 & = & [35,135,190,195,198] \\
H\cdot 10 & = & [10,126,182,200,235] & H\cdot 53 & = & [53,56,61,116,216] \\
H\cdot 16 & = & [16,51,69,125,241] & H\cdot 41 & = & [41,67,85,115,194] \\
H\cdot 11 & = & [11,133,150,220,239] & H\cdot 57 & = & [57,136,166,184,210] \\
H\cdot 12 & = & [12,31,101,118,240] & H\cdot 43 & = & [43,90,107,130,132] \\
H\cdot 14 & = & [14,29,54,76,78] & H\cdot 119 & = & [119,121,144,161,208] \\
H\cdot 173 & = & [173,175,197,222,237] & H\cdot 45 & = & [45,65,66,147,179] \\
H\cdot 15 & = & [15,22,49,189,227] & H\cdot 72 & = & [72,104,185,186,206] \\
H\cdot 24 & = & [24,62,202,229,236] & H\cdot 68 & = & [68,83,92,105,154] \\
H\cdot 17 & = & [17,23,89,164,209] & H\cdot 97 & = & [97,146,159,168,183]
\end{array}
$$

We give two SDSs with parameters $(251; 125, 120, 115, 115; 224)$, via the index sets J, K, L, M (with respective cardinalities $25, 24, 23, 23$) to be used in (1), which give rise to Hadamard matrices of order $4 \cdot 251 = 1004$. The associated decomposition into the sum of 4 squares is:

$$
\begin{array}{rcl}
4\cdot 251 = 1004 & = & 1^2 + 11^2 + 21^2 + 21^2 = \\
 & = & (251 - 2\cdot 125)^2 + (251 - 2\cdot 120)^2 + (251 - 2\cdot 115)^2 + (251 - 2\cdot 115)^2.
\end{array}
$$

$$
\begin{aligned}
J &= \{2,4,5,6,7,111,9,37,10,11,12,14,173,15,24,74,19,48,33,73,53,57,43,72,68\} \\
K &= \{2,55,6,75,16,11,173,24,17,42,18,19,106,21,30,48,34,73,35,53,41,57,43,97\} \\
L &= \{1,2,4,50,6,75,9,37,10,11,173,15,17,18,21,48,36,34,119,45,72,68,97\} \\
M &= \{32,2,25,3,5,8,7,16,173,15,74,19,106,21,95,30,73,53,41,57,45,72,68\}
\end{aligned}
$$

$$
\begin{aligned}
J &= \{32,3,55,50,5,6,7,9,37,11,12,14,15,24,18,19,82,30,36,34,73,35,41,57,72\} \\
K &= \{1,32,25,55,5,8,75,9,37,11,14,15,24,17,42,18,19,95,48,41,57,43,45,97\} \\
L &= \{1,2,25,3,50,8,75,9,11,12,173,24,17,28,95,30,33,36,34,73,45,72,97\} \\
M &= \{32,25,4,5,6,75,7,16,11,12,24,42,106,28,95,48,73,35,53,41,57,45,72\}
\end{aligned}
$$

3.3 $v = 631$

Consider the subgroup $H = \{1,8,43,64,79,188,228,242,279,310,339,344,512,562,587\}$ of order 15, of $Z^{\star}_{631}$. Here are the 42 nontrivial orbits of the action of H on Z_{631}.

$$
\begin{aligned}
H\cdot 1 &= \{1,8,43,64,79,188,228,242,279,310,339,344,512,562,587\} \\
H\cdot 2 &= \{2,16,47,57,86,128,158,376,393,456,484,493,543,558,620\} \\
H\cdot 3 &= \{3,24,53,95,129,192,206,237,274,299,386,401,424,499,564\} \\
H\cdot 4 &= \{4,32,94,114,121,155,172,256,281,316,337,355,455,485,609\} \\
H\cdot 5 &= \{5,36,40,133,215,286,288,309,320,395,411,433,458,509,579\} \\
H\cdot 6 &= \{6,48,106,141,171,190,217,258,367,384,412,474,497,548,598\} \\
H\cdot 7 &= \{7,54,56,60,148,277,301,323,334,429,432,448,480,515,553\} \\
H\cdot 9 &= \{9,10,72,80,159,191,235,266,285,387,430,527,572,576,618\} \\
H\cdot 11 &= \{11,73,88,138,147,175,238,255,473,503,545,574,584,615,629\} \\
H\cdot 12 &= \{12,96,103,137,193,212,282,317,342,363,380,434,465,516,565\} \\
H\cdot 13 &= \{13,55,59,104,201,244,346,365,396,440,472,551,559,621,622\} \\
H\cdot 14 &= \{14,15,37,108,112,120,227,233,265,296,329,399,475,554,602\} \\
H\cdot 17 &= \{17,41,81,84,89,90,100,136,169,222,326,328,457,501,514\} \\
H\cdot 18 &= \{18,20,143,144,160,229,318,382,423,470,513,521,532,570,605\} \\
H\cdot 19 &= \{19,131,152,181,186,211,226,239,253,263,417,426,546,582,585\} \\
H\cdot 21 &= \{21,25,34,82,162,168,178,180,200,272,283,338,371,397,444\} \\
H\cdot 22 &= \{22,146,176,276,294,315,350,375,459,476,510,517,537,599,627\} \\
H\cdot 23 &= \{23,107,184,189,196,210,225,250,306,340,358,418,518,538,555\} \\
H\cdot 26 &= \{26,61,99,110,118,161,208,249,313,402,471,487,488,611,613\} \\
H\cdot 27 &= \{27,28,30,74,167,216,224,240,319,454,466,477,530,573,592\} \\
H\cdot 29 &= \{29,77,156,232,302,335,366,398,404,511,519,523,594,616,617\} \\
H\cdot 31 &= \{31,71,91,97,127,145,149,248,385,413,446,529,556,561,568\} \\
H\cdot 33 &= \{33,83,134,157,219,247,264,373,414,441,460,490,525,583,625\} \\
H\cdot 35 &= \{35,51,109,123,241,243,252,267,270,280,300,347,353,408,507\} \\
H\cdot 38 &= \{38,203,221,262,304,362,372,422,452,461,478,506,526,533,539\} \\
H\cdot 39 &= \{39,58,101,154,165,177,312,391,407,415,464,557,601,603,604\} \\
H\cdot 42 &= \{42,45,50,68,111,163,164,257,324,336,356,360,400,544,566\} \\
H\cdot 44 &= \{44,69,119,287,292,321,352,389,403,443,552,567,588,623,630\} \\
H\cdot 46 &= \{46,49,85,205,214,368,378,392,405,420,445,450,479,500,612\}
\end{aligned}
$$

$$
\begin{aligned}
H \cdot 52 &= \{52,122,173,198,220,236,311,322,343,345,416,498,591,595,626\}\\
H \cdot 62 &= \{62,139,142,182,194,195,254,261,290,298,427,481,491,496,505\}\\
H \cdot 63 &= \{63,70,75,102,185,218,246,383,482,486,504,534,540,560,600\}\\
H \cdot 65 &= \{65,87,231,271,275,295,307,374,467,468,520,563,581,586,589\}\\
H \cdot 66 &= \{66,115,166,197,251,268,289,314,349,419,438,494,528,535,619\}\\
H \cdot 67 &= \{67,132,207,230,245,332,357,394,425,439,502,536,578,607,628\}\\
H \cdot 76 &= \{76,93,113,213,273,291,325,381,406,421,435,442,447,524,608\}\\
H \cdot 78 &= \{78,116,151,183,199,202,297,308,330,354,483,571,575,577,624\}\\
H \cdot 92 &= \{92,98,105,125,153,170,179,209,259,269,327,369,410,428,593\}\\
H \cdot 117 &= \{117,130,174,303,305,409,462,495,531,541,542,547,550,590,614\}\\
H \cdot 124 &= \{124,223,278,284,331,351,361,364,379,388,390,508,522,580,596\}\\
H \cdot 126 &= \{126,135,140,150,204,333,341,370,377,436,437,449,489,492,569\}\\
H \cdot 187 &= \{187,234,260,293,348,359,431,451,453,463,469,549,597,606,610\}
\end{aligned}
$$

We give four nonequivalent SDSs with parameters $(631; 315, 330, 330, 330; 674)$, via their index sets J, K, L, M (with respective cardinalities $21, 22, 22, 22$) to be used in (1), which give rise to Hadamard matrices of order $4 \cdot 631 = 2524$. In addition, the first two SDSs give rise to skew-Hadamard matrices of order $4 \cdot 631 = 2524$. The associated decomposition into the sum of 4 squares is:

$$
\begin{aligned}
4 \cdot 631 = 2524 &= 1^2 + 29^2 + 29^2 + 29^2 = \\
&= (631 - 2 \cdot 315)^2 + (631 - 2 \cdot 330)^2 + (631 - 2 \cdot 330)^2 + (631 - 2 \cdot 330)^2.
\end{aligned}
$$

$$
\begin{aligned}
J &= \{1,2,3,4,6,7,12,13,14,17,19,21,26,27,31,38,42,52,62,76,124\}\\
K &= \{1,2,3,4,5,6,7,9,12,17,23,26,27,31,33,38,42,44,52,76,78,126\}\\
L &= \{1,2,3,4,6,7,9,11,12,13,14,17,18,19,21,29,35,46,52,62,66,76\}\\
M &= \{1,2,3,4,5,6,12,13,14,18,19,21,22,26,27,38,39,42,63,67,92,124\}
\end{aligned}
$$

$$
\begin{aligned}
J &= \{11,13,19,22,26,29,31,33,38,39,44,52,62,65,66,67,76,78,117,124,187\}\\
K &= \{1,3,4,5,9,11,14,17,18,22,23,26,29,33,38,39,42,46,62,65,67,117\}\\
L &= \{1,2,5,6,9,17,18,21,22,27,33,39,44,46,52,66,76,78,92,117,124,187\}\\
M &= \{2,4,5,7,9,11,12,13,18,19,21,23,29,31,42,44,65,66,67,78,92,187\}
\end{aligned}
$$

$$
\begin{aligned}
J &= \{1,3,4,7,12,13,17,18,19,27,29,31,33,35,42,46,62,67,92,124,187\}\\
K &= \{5,6,7,9,12,17,18,21,22,26,29,33,35,38,42,44,62,63,67,76,124,126\}\\
L &= \{4,6,7,9,11,13,14,17,18,21,22,23,27,29,35,39,46,67,78,124,126,187\}\\
M &= \{2,5,6,7,11,13,14,18,19,21,27,29,33,35,39,44,52,62,63,65,117,187\}
\end{aligned}
$$

$$
\begin{aligned}
J &= \{1,2,4,5,6,9,11,12,13,17,22,27,29,42,44,65,78,92,117,126,187\}\\
K &= \{1,7,9,13,17,19,22,23,27,29,31,33,35,38,44,46,65,66,76,78,126,187\}\\
L &= \{2,3,4,5,13,17,21,22,29,35,38,39,52,62,63,65,67,76,92,117,124,126\}\\
M &= \{2,3,4,5,7,9,11,12,17,18,21,22,29,33,42,44,46,52,65,66,92,187\}
\end{aligned}
$$

4 Acknowledgements

The first and the third author wish to acknowledge generous support by NSERC. This work was made possible by the facilities of the Shared Hierarchical Academic Research Computing Network (SHARCNET) and Compute Ontario, as well as the facilities of the Réseau Québécois de Calcul de Haute Performance (RQCHP) and Calcul Québec.

References

[1] C. Colbourn, J. Dinitz, Handbook of Combinatorial Designs, Second Edition, CRC Press, 2006.

[2] D. Ž. Đoković, Hadamard matrices of order 764 exist. Combinatorica 28 (2008), no. 4, 487–489.

[3] D. Ž. Đoković, Skew-Hadamard matrices of orders 436, 580, and 988 exist. J. Combin. Des. 16 (2008), no. 6, 493–498.

[4] D. Ž. Đoković, Hadamard matrices of small order and Yang conjecture. J. Combin. Des. 18 (2010), no. 4, 254–259.

[5] D. Ž. Đoković, Cyclic $(v; r, s; \lambda)$ difference families with two base blocks and $v \leq 50$. Ann. Comb. 15 (2011), no. 2, 233–254.

[6] D. Ž. Đoković, Small orders of Hadamard matrices and base sequences, Intl. Math. Forum vol. 6, no. 62, (2011), pp. 3061–3067.

[7] K. J. Horadam, Hadamard matrices and their applications. Princeton University Press, Princeton, NJ, 2007.

[8] K. J. Horadam, Hadamard matrices and their applications: progress 2007–2010. Cryptogr. Commun. 2 (2010), no. 2, 129–154.

[9] H. Kharaghani, B. Tayfeh-Rezaie, A Hadamard matrix of order 428. J. Combin. Des. 13 (2005), no. 6, 435–440.

[10] J. Seberry, M. Yamada, Hadamard matrices, sequences, and block designs. In Contemporary design theory, 431–560, Wiley-Intersci. Ser. Discrete Math. Optim., Wiley, New York, 1992,